IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF:
35 WAYCROSS DRIVE, FIELDALE,
VIRGINIA 24089

Case No. 7:23mj58

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Francesco Boccieri, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 35 Waycross Drive, Fieldale, Virginia 24089, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and have been since 2007. I am a graduate of the Federal Law Enforcement Training Center (FLETC) and the ATF Special Agent Basic Training Academy. I have received specialized training in various aspects of criminal law enforcement relating to arson, explosives, narcotics and firearms investigations. As a duly sworn federal law enforcement agent, I am authorized to carry firearms, execute warrants, and make arrests for offenses against the United States and to perform such other duties as authorized by law. I am familiar with federal criminal laws pertaining to narcotics offenses under Title 21 of the United States Code and firearms offenses under Titles 18 and 26 of the United States Code.

5/12/2023

Prior to joining the ATF, I was a police officer with the United States Capitol Police for approximately five years. I have participated in the execution of numerous arrest and search warrants for criminal offenses involving narcotics and illegal possession of firearms. I also have received training on cellular phone and computer forensics and have extensive experience extracting and analyzing data from electronic devices.

3. The facts in this affidavit come from my training and experience as well as information obtained from other law enforcement officers and interviews with witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

4. This affidavit is submitted in support of a warrant to authorize the search of the residence located at 35 Waycross Drive, Fieldale, Virginia, in the Western District of Virginia, as more particularly described in Attachment A, which may constitute or contain records, fruits, instrumentalities and evidence of violations of Title 18, United States Code, Sections 1341, 1343, 1344, as well as 18 U.S.C. § 3147. This is a residence of Herman Lee ESTES, Jr. ESTES has resided at this address for over 13 months, according to the United States Probation Office. Henry County, Virginia GIS website e911 data indicates the property is owned by Clyde Newby Jr. c/o Cynthia A. Hairston.

5. The applied-for warrant would authorize the search of this property for the

5/12/2023

purpose of identifying evidence, fruits and instrumentalities of violations of the federal laws, as described more particularly in Attachment B.

PROBABLE CAUSE

6. Herman Lee ESTES, Jr. was indicted by a federal grand jury on September 17, 2020, on one count of knowingly possessing a firearm after previously having been convicted of a felony, in violation of 18 U.S.C. § 922(g)(1). *See United States v. Estes*, Case No. 4:20cr00024 (W.D. Va.).

7. Following a detention hearing held on April 8, 2022, ESTES was released on a $15,000 unsecured bond into the custody of his wife, Tia Estes, to live at 35 Waycross Drive in Fieldale, Virginia. One of his conditions of release prohibits ESTES from violating any federal, state or local crime while on supervision.

8. On or about January 17, 2023, ESTES reached out to Joshua Desforges, a realtor at MKB Realtors, via Zillow about a property in Boones Mill, Virginia listed for sale at approximately $775,000. ESTES told Desforges that his budget was around $1.5 million. ESTES told Desforges that he traded bonds through his estate/trust. He provided Desforges with what ESTES represented to be an IRS tax transcript purportedly showing ESTES's income to be $32 million, with an anticipated tax refund of $18 million, which ESTES explained would be transferred to his estate as part of a trust. Based on ESTES's representations, Desforges showed ESTES a listing for a property at 7419 Old Mill Plantation Drive in Roanoke, Virginia, which was listed for sale at the time at $1.2 million.

RBB 5/12/2023

The property, which was newly constructed, was owned by Quality Development Group LLC. ESTES met Desforges at the property for a viewing.

9. On January 25, 2023, ESTES entered a plea of guilty to the § 922(g) charge. He was continued on the same terms and conditions of pretrial release pending sentencing.

10. In approximately the middle of March, 2023, ESTES contacted Desforges again and told him that his $18 million tax refund had cleared. Desforges arranged another viewing of the Old Mill Plantation property for ESTES and his family. Desforges prepared a cash offer for 7419 Old Mill Plantation Drive at ESTES's request. ESTES provided as proof of funds for the cash offer contract what he represented to be a commitment letter from

5/12/2023

FundSmart, with a stated address of 5027 W Laurel St, Tampa, FL 33607 and phone number of (813) 358-0381. The letter is dated "March 29th, 2023" and the body of the letter reads:

To Whom it May Concern:

This letter is to inform you that HERMAN LEE ESTES ESTATE has been approved for a private real estate loan in the amount of $1315000 for the purchase of 7419 Old Mill Plantation Dr., Roanoke, Virginia 24018. This approval is subject to the following conditions:

- Review and approval of ALTA Title report on the subject property.
- Subject to final underwriting.

FundSmart is prepared to close this transaction within 2 business days of obtaining and approving the ALTA Title Commitment. This Approval expires on April 29th, 2023.

Please contact the undersigned directly with questions or concerns.

Regards,

FundSmart
Private Lender
(813) 358-0381

11. An open source search of FundSmart's purported address of 5027 W Laurel St, Tampa, FL 33607 shows a building at this location, but the signs are for an active business operating under the name Residential Acceptance Corporation. A search of Florida business records through the Florida Department of State, Division of Corporations' website shows a business operating under the name FundSmart Financial LLC with a registered address of 7901 4th Street N Suite 300, St. Petersburg, FL 33702 and no activity prior to March 22, 2023. This St. Petersburg address shows a business operating under the

5/12/2023

name Resident Agent Services—not FundSmart. Calls to (813) 358-0381, the number listed on the FundSmart letter, go straight to voicemail.

12. ESTES also referred Desforges to an individual named "Daniel" LNU, whom ESTES represented to be the manager for ESTES's trust. Desforges called "Daniel" at phone number (470) 257-2505, the number provided by ESTES. "Daniel" told Desforges that FundSmart was the holder of ESTES's trust. "Daniel" also told Desforges that he was the manager of ESTES' trust and, as such, had to approve the purchase of 7419 Old Mill Plantation Drive using trust funds. After asking a few questions, he gave his approval to Desforges.

13. Because the contract was for a cash offer, there was no inspection and no appraisal conducted of the property. The seller accepted ESTES's offer and the contract was ratified on March 29, 2023.

14. Homestead Settlement Services conducted the closing of the real estate transaction. ESTES primarily communicated with Homestead via email using the address hermanestes98@gmail.com. Some communications were conducted using Qualia, Homestead's secure email client, which allowed for email, secure file sharing and electronic signing of documents.

15. ESTES provided Homestead with a "Registered Bonded Promissory Note" in the amount of $1,307,199.43, as well as a series of documents that purport to be related to his estate and/or trust. These documents appear to the undersigned to be fraudulent. For

5/12/2023

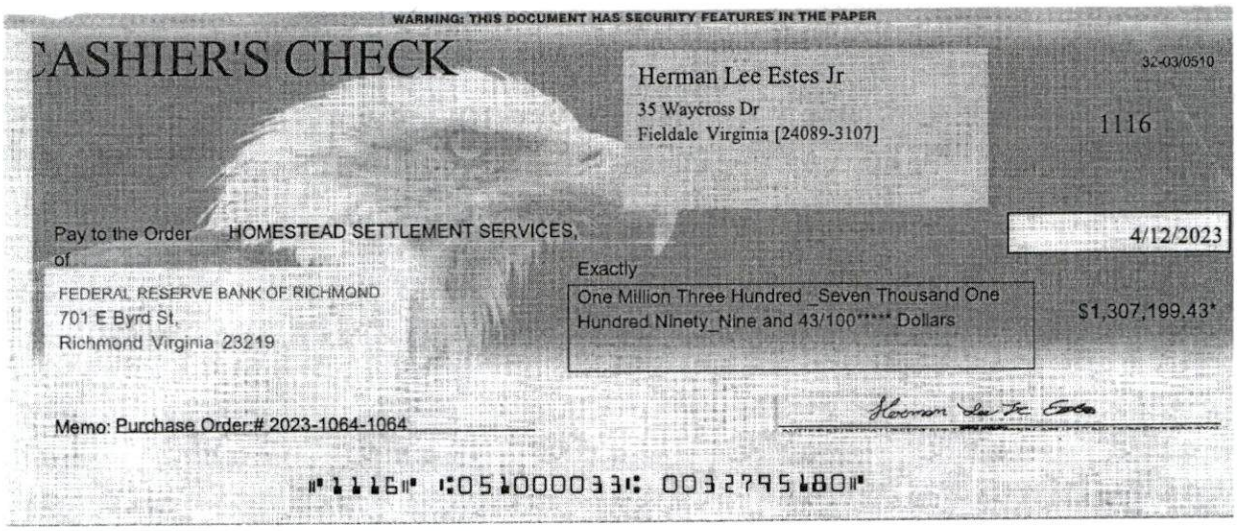
example, one of these documents purports to be an IRS tax document Standard Form 28 but lists ESTES's home address as 1906 Belleview Avenue, Roanoke, Virginia, which is the address for Carilion Roanoke Memorial Hospital. Another purported IRS document, Form 56, misspells the word "fiduciary" in the header. Another document references ESTES's fiduciary's name as Janet Yellen, the current U.S. Secretary of the Treasury and previous chair of the Federal Reserve. One document lists account and routing numbers for various Federal Reserve Banks and other financial institutions, including the Treasury Direct routing number and account number. One document titled "Affidavit of Individual Surety" lists ESTES's address as 1906 Belleview Avenue and his employer as "Department of Treasury, IRS." This document also lists as the assets pledged in support of the attached bond as: "Private registered bond for setoff non-negotiable value: $100,000,000,000.00 (One Hundred Billion) US Dollars RE Certificate of Live Birth #145-83-052234 accepted for value and exempt from levy deposited to US Treasury and charged to Herman Lee Jr Estes and 145-83-052234, issue date: May 29th, 2023, Bond Number E32795180." Several of these documents appear to have been notarized.

16. Homestead required either a wire transfer or a cashier's check for the cash purchase of 7419 Old Mill Plantation Drive. ESTES asked to do an ACH withdrawal, rather than a wire transfer, and Homestead declined. The parties agreed to proceed with a cashier's check. ESTES sent a purported cashier's check from FedEx OnSite at the Dollar General in Fieldale, Virginia on April 12, 2023 at 9:34am. Surveillance video from April 12, 2023 at

5/12/2023

approximately 9:30am obtained from the Dollar General shows an individual recognized by the undersigned to be ESTES purchasing envelopes and placing what appears to be the check inside one of the envelopes, before affixing the FedEx label and handing it to the cashier. The check was delivered to Homestead Settlement Services in Roanoke, Virginia on April 13, 2023 at 9:08am.

17. The check, which appears to be drawn off the Federal Reserve Bank of Richmond in the amount of $1,307,199.43, is signed by ESTES:



18. ESTES explained to Homestead that he was a sovereign citizen and that he did not deal with public banks. He further stated that he was his own personal banker and that he dealt directly with the Federal Reserve Bank.

5/12/2023

19. Based on my training and experience, I know that sovereign citizens are a loosely affiliated group of individuals who claim that the federal government has no authority over them. They perpetuate schemes that fraudulently purport to eliminate debts or reverse foreclosures. They often use trusts, including Unincorporated Business Organization Trusts, alias names, and names of third parties to title property and hide assets. Based on their claimed sovereign citizen status, they do not file tax returns or pay taxes that are owed. Sovereign citizens adhering to the redemption scheme write bogus checks, such as the one signed by ESTES above, in attempts to pay debts. The redemption scheme purports that Treasury accounts exist for all U.S. citizens and that these funds can be accessed to pay taxes and other debts. They often sign documents for other sovereigns who are utilizing the same scheme. Sovereign citizens are known to operate throughout the country and overseas and to communicate with other like-minded sovereign citizens about their ideologies, schemes, and related legal issues. Sovereign citizen ideologies are often promoted through seminars, websites, podcasts, and word of mouth.

20. The Federal Reserve Bank of Richmond has confirmed that the check sent by ESTES to Homestead is fraudulent.

5/12/2023

21. The check was deposited by Homestead to its American National Bank and Trust account number ending in 6201 on April 13, 2023. Bank records show $1,307,199.43 was credited to the account on April 13, 2023.

22. On April 13, 2023 at 10:52 a.m., Allison Robins from Homestead emailed Robin Jeffries at American National Bank and Trust to inquire as to whether ESTES's cashier's check had been processed and cleared. In her email, Allison Robins stated that she did not want to record the deed until the check cleared. Robin Jeffries responded via email at 4:01 p.m. on April 13, 2023, and stated the check would show up on Homestead's balance the following day, adding "since it is a cashier's check, it's just like depositing cash—once it's there, it's clear….." Robins checked Homestead's account balance and saw the $1,307,199.43 credited to the account. As such, they proceeded to closing.

23. Closing for the sale of the 7419 Old Mill Plantation Drive was held on Friday, April 14, 2023. The necessary documents for the transfer of the property to ESTES were signed, and the deed was recorded with the Roanoke County Clerk's Office the same day.

24. On Monday, April 17, 2023, American National Bank and Trust account records show that $1,307,199.43 was debited from Homestead's account. American National Bank and Trust notified Homestead that the check was returned fraudulent.

25. On April 17, 2023, Desforges called ESTES to tell him his check had bounced. ESTES told Desforges that cashier's checks cannot bounce. Two days later, ESTES called Desforges to inquire about the locks being changed on the Old Mill Plantation

5/12/2023

Drive residence. Desforges told ESTES the money was not there. ESTES told Desforges to contact his representative at the bank, Janet Yellen.

26. On April 21, 2023, the United States Probation Office conducted a home visit at 7419 Old Mill Plantation Drive. Probation reported that ESTES and his family were living in the house but that the furnishings were limited to two air mattresses and some personal items. The balance of the family's furnishings and belongings remained at his 35 Waycross Drive, Fieldale, Virginia residence. ESTES informed Probation that he is currently splitting time between both residences. Probation further reported that during the home visit, ESTES had a silver laptop computer with him, which according to probation he always carries, as well as a yellow backpack next to the fireplace in the Old Mill Plantation Drive residence that is full of paperwork. Probation provided a photograph of ESTES's open laptop computer, which had a document appearing to be a go-by for sovereign citizens.

27. According to the Presentence Report prepared by probation in connection with *United States v. Estes*, Case. No. 4:20cr00024, ESTES reported earning $250,000 per year plus bonuses from various companies. None of the financial or employment information provided by ESTES to probation could be verified.

28. There is probable cause to believe that the property to be searched will contain evidence that ESTES engaged in violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud) and 1344 (bank fraud), as well as 18 U.S.C. § 3147 (offense committed on pretrial release). The evidence outlined above demonstrates that ESTES devised a scheme to

5/12/2023

defraud the parties to the sale of the Old Mill Plantation Drive property and, for the purpose of executing that scheme, he caused to be transmitted by means of a wire false representations about his source of cash funds to purchase the property, used a private and commercial interstate carrier of mail material (FedEx) to deliver a fraudulent check purported to be drawn off the Federal Bank of Richmond to the closing company as payment for that property, and caused that fraudulent check to be deposited at a financial institution. By violating these federal laws, ESTES knowingly disobeyed the court's order setting conditions of pretrial release in the case of *United States v. Estes*, No. 4:20cr00024 (W.D. Va.).

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic

5/12/2023

storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

RSB 5/12/2023

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of documents and evidence related to this investigation, I am aware that computer equipment was used to generate, store, and print documents used in ESTES's scheme to fraudulently obtain ownership rights to and take possession of 7419 Old Mill Plantation Drive. There is reason to believe that there may be a computer currently located on the PREMISES, because the majority of ESTES's belongings remain at the PREMISES, and ESTES is known to carry a laptop computer with him.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the

82803
5/12/2023

crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus

5/12/2023

enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a

RBS 5/12/2023

computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about

5/12/2023

how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to

5/12/2023

make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a

0803
5/12/2023

search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

35. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers

RSB 5/12/2023

or storage media, the warrant applied for would permit the seizure and review of those items as well.

36. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home"

5/12/2023

button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

JLS 5/12/2023

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

5/12/2023

g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the PREMISES and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

h. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from any person whose device is to be searched to display any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices, including to (1) press or swipe the fingers (including thumbs) of those

RSB 5/12/2023

persons to the fingerprint scanner of the devices found at the PREMISES; (2) hold the devices found at the PREMISES in front of the face of those persons to activate the facial recognition feature; and/or (3) hold the devices found at the PREMISES in front of the face of those persons to activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

i. The proposed warrant does not authorize law enforcement to require that the persons whose device is to be searched state or otherwise provide the password, or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel those persons to state or otherwise provide that information. However, the voluntary disclosure of such information by those persons would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask any of those persons for the password to any devices, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any devices, the agents will not state or otherwise imply that the warrant requires the person to provide such information and will make clear that

5/12/2023

providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

37. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,

FRANCESCO BOCCIERI
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me
on May 12, 2023:

UNITED STATES DISTRICT JUDGE